**English translation of JP 2001-86110 dated 3/30/2001 (a portion thereof)

DETAILED DESCRIPTION OF THE INVENTION

TECHNICAL FIELD

The present invention relates to a packet communication system of encrypted information, and more particularly, to a packet communication system of encrypted information treating encrypted/decrypted information using a streaming encryption system.

BACKGROUND ART

Streaming encryption systems are known as encryption systems available to high speed packet data communications. In a streaming encryption system, pseudo-random numbers are generated rendering a prescribed encryption key as default, and the system encrypts the sending information sequentially by a bit unit. When using a streaming encryption system in packet data communication, parts of the encrypted information is stored in packets and sent.

On the one hand, in the case of implementing the encrypted communication using a streaming encryption system, decryption becomes relatively easy because of commonalities in the encrypted information when encrypting multiple information with the same encryption key fixing, resulting in decline of encryption strength. Therefore, it has been conventionally known that the encryption key is changed periodically when using a streaming encryption system.

BRIEF SUMMARY OF THE INVENTION

However, in a streaming encryption system, it is necessary to use the same encryption key between a sender who encrypts information and a receiver who decrypts imformation. Accordingly, changing the encryption key for both sides has to be synchronized between them. On the other hand, when changing the encryption key frequently to increase encryption strength, it causes another problem that changing the encryption key adds greater load to hardware and increases the possibility of desynchronization.

To avoid these problems described above regarding such synchronization as illustrated in figure 9, there is a way for inserting timing signals indicating the change of encryption within a particular packet. By changing the encryption key in time by detecting these timing signals on the receiver side, there is no need to be synchronized between the sender and the receiver. However, according to this method, there is still a problem that the receiver has to administer the encryption key which is being changed sequentially beforehand, as well as requiring a device configured to detect the timing signals.

Therefore, the present invention has an objective of providing a packet communication system of encrypted information which can implement the change of the encryption key and overcome the problem of synchronization by being without synchronization for changing the encryption key.

The present invention has another objective of providing packet communication system of encrypted information without management of the encryption key by a receiver.

To achieve the objectives as described above, the packet communication system of the present invention is configured with a packet sending device and a packet receiving device as described below. That is, the packet sending device is configured to comprise means for generating a packet, wherein the sending information is divided into a plurality of packets, means for stream encrypting the packet, wherein the encryption generates pseudo-random numbers rendering one of the plurality of an encryption key as default which is changed in every packet, and which encrypts parts of information sequentially by a bit unit which is stored in the plurality of packets using pseudo-random numbers, means for storing the encryption key used by the encryption within the packet which stores parts of the encrypted information, and means for sequentially sending parts of the encrypted information and packets which store the encryption key.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－86110
（P2001－86110A）
(43)公開日　平成13年３月30日(2001.3.30)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/18		Ｈ０４Ｌ　9/00	６５１	５Ｊ１０４
9/08			６０１Ｃ	５Ｋ０３０
12/56		11/20	１０２Ｚ	

審査請求　未請求　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願平11－258447

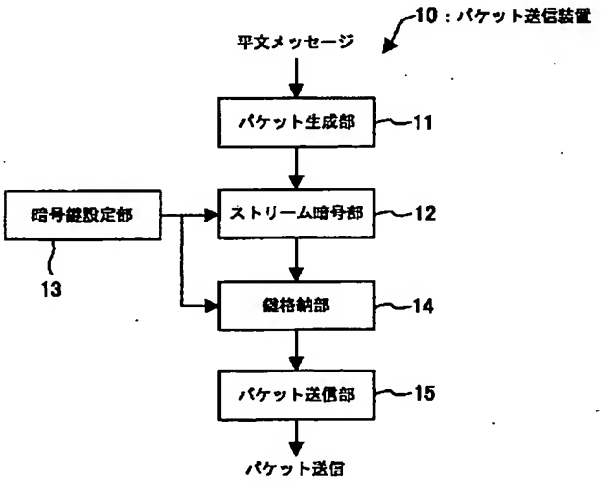
(22)出願日　平成11年９月13日(1999.9.13)

(71)出願人　000003104
東洋通信機株式会社
神奈川県高座郡寒川町小谷２丁目１番１号
(72)発明者　力石　徹也
神奈川県高座郡寒川町小谷２丁目１番１号
東洋通信機株式会社内
(74)代理人　100098039
弁理士　遠藤　恭

Ｆターム(参考)　5J104 AA01 AA16 AA34 EA02 JA04
NA02 NA04 NA23 NA37 PA00
5K030 GA14 GA15 JA05 KA17

(54)【発明の名称】　暗号化情報のパケット通信システム

(57)【要約】
【課題】　暗号鍵の変更の同期を必要とせずに、暗号鍵の変更を実現した暗号化情報のパケット通信システムを提供する。
【解決手段】　本発明におけるパケット送信装置は、送信する情報を、複数のパケットにするパケット生成手段１１と、前記パケット毎に変更される複数の暗号鍵のうちの一つを初期値として疑似乱数列を生成し、該疑似乱数列を用いて前記複数のパケットに格納される情報の部分を順次ビット単位で暗号化するストリーム暗号化手段１２と、前記暗号化された情報の部分を格納したパケット内に、該暗号に用いられた暗号鍵を格納する鍵格納手段１４と、前記暗号化された情報の部分及び前記暗号鍵を格納したパケットを、順次送信するパケット送信手段１５とを備える。



【特許請求の範囲】

【請求項１】　送信する情報を、複数のバケットにするバケット生成手段と、
前記バケット毎に変更される複数の暗号鍵のうちの一つを初期値として疑似乱数列を生成し、該疑似乱数列を用いて前記複数のバケットに格納される情報の部分を順次ビット単位で暗号化するストリーム暗号化手段と、
前記暗号化された情報の部分を格納したバケット内に、該暗号に用いられた暗号鍵を格納する鍵格納手段と、
前記暗号化された情報の部分及び前記暗号鍵を格納したバケットを、順次送信するバケット送信手段と、を備えたことを特徴とする暗号化情報のバケット送信装置。

【請求項２】　送信する情報を、複数のバケットにするバケット生成手段と、
所定数の前記バケット毎に変更される複数の暗号鍵のうちの一つを初期値として疑似乱数列を生成し、該疑似乱数列を用いて前記複数のバケットに格納される情報の部分を順次ビット単位で暗号化するストリーム暗号化手段と、
前記暗号化された情報の部分を格納した、連続して送信される前記所定数のバケット内に、該暗号に用いられた暗号鍵を、該暗号鍵を構成するビットで分割して格納する鍵格納手段と、
前記暗号化された情報の部分及び前記暗号鍵の部分を格納したバケットを、順次送信するバケット送信手段と、を備えたことを特徴とする暗号化情報のバケット送信装置。

【請求項３】　請求項１記載のバケット送信装置からのバケットを順次受信するバケット受信手段と、
前記受信したバケットから前記暗号鍵を抽出する暗号鍵抽出手段と、
前記抽出した暗号鍵を初期値として疑似乱数列を生成し、該疑似乱数列を用いて前記バケットに格納される情報の部分を順次ビット単位で復号化するストリーム復号化手段と、を備えたことを特徴とするバケット受信装置。

【請求項４】　請求項２記載のバケット送信装置からのバケットを順次受信するバケット受信手段と、
前記受信した所定数のバケットから前記暗号鍵の部分を抽出する暗号鍵抽出手段と、
前記抽出した暗号鍵の部分から元の暗号鍵を生成する暗号鍵生成部と、
前記生成された暗号鍵を初期値として疑似乱数列を生成し、該疑似乱数列を用いて前記所定数のバケットに格納される情報の部分を順次ビット単位で復号化するストリーム復号化手段と、を備えたことを特徴とするバケット受信装置。

【請求項５】　請求項１記載のバケット送信装置と、請求項３記載のバケット受信装置で構成されるバケット通信システム。

【請求項６】　請求項２記載のバケット送信装置と、請求項４記載のバケット受信装置で構成されるバケット通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化情報のバケット通信システムに関し、特に、ストリーム暗号方式を用いて暗号化・復号化される情報を取り扱う暗号化情報のバケット通信システムに関する。

【０００２】

【従来の技術】高速なバケットデータ通信に利用可能な暗号化方式として、ストリーム暗号方式が知られている。ストリーム暗号方式では、所定の暗号鍵を初期値として疑似乱数列を生成し、この擬似乱数列を用いて、送信する情報を順次ビット単位で暗号化する。バケットデータ通信においてストリーム暗号方式を用いる場合、暗号化された情報の部分をバケットに格納し送信する。

【０００３】一方で、ストリーム暗号方式を用いて暗号通信を実現する場合、一つの暗号鍵に固定したままで多数の情報を暗号化していると、該暗号化された情報の共通性から暗号の解読が比較的容易になり、暗号強度が低下するという問題がある。このため従来から、ストリーム暗号方式を用いる場合は、暗号鍵を周期的に変更することが行われている。

【０００４】

【発明が解決しようとする課題】しかしながら、ストリーム暗号方式においては、情報の暗号化側、すなわち送信者側と、情報の復号化側、すなわち受信者側で、同じ暗号鍵を用いる必要があることから、同期を取って双方の暗号鍵を変更しなければならない。ところが、暗号強度を高めるために暗号鍵の変更を頻繁に行った場合、同期ずれの危険性が高まり、また暗号鍵の変更の際のハードウェア負荷が大きくなるという問題がある。

【０００５】また、このような同期に伴う問題を回避するために、図９に示すように、特定のバケット内に、暗号の変更を示すタイミング信号を挿入する方法がある。受信側では、このタイミング信号を検出し、これを境にして使用する暗号鍵を変更することにより、同期を不要としている。しかしながら、この方法によれば、前記タイミング信号を検出するための装置構成が必要となると共に、順次変更する暗号鍵は、依然として予め受信側で管理しなければならないという問題がある。

【０００６】従って本発明の目的は、暗号鍵の変更の同期を必要とせずに、暗号鍵の変更を実現し、前記同期に伴う問題を回避した暗号化情報のバケット通信システムを提供することにある。

【０００７】本発明の別の目的は、受信側における暗号鍵の管理を不要とした暗号化情報のバケット通信システムを提供することにある。

【０００８】

【課題を解決するための手段】上記目的を達成するため本発明のパケット通信システムは、下記パケット送信装置及びパケット受信装置で構成される。すなわち本発明のパケット送信装置は、送信する情報を、複数のパケットにするパケット生成手段と、前記パケット毎に変更される複数の暗号鍵のうちの一つを初期値として疑似乱数列を生成し、該疑似乱数列を用いて前記複数のパケットに格納される情報の部分を順次ビット単位で暗号化するストリーム暗号化手段と、前記暗号化された情報の部分を格納したパケット内に、該暗号に用いられた暗号鍵を格納する鍵格納手段と、前記暗号化された情報の部分及び前記暗号鍵を格納したパケットを、順次送信するパケット送信手段とを備えて構成される。

【０００９】一方、本発明のパケット受信装置は、前記パケット送信装置からのパケットを順次受信するパケット受信手段と、前記受信したパケットから前記暗号鍵を抽出する暗号鍵抽出手段と、前記抽出した暗号鍵を初期値として疑似乱数列を生成し、該疑似乱数列を用いて前記パケットに格納される情報の部分を順次ビット単位で復号化するストリーム復号化手段とを備えて構成される。

【００１０】また、本発明のパケット送信装置は、送信する情報を、複数のパケットにするパケット生成手段と、所定数の前記パケット毎に変更される複数の暗号鍵のうちの一つを初期値として疑似乱数列を生成し、該疑似乱数列を用いて前記複数のパケットに格納される情報の部分を順次ビット単位で暗号化するストリーム暗号化手段と、前記暗号化された情報の部分を格納した、連続して送信される前記所定数のパケット内に、該暗号に用いられた暗号鍵を、該暗号鍵を構成するビットで分割して格納する鍵格納手段と、前記暗号化された情報の部分及び前記暗号鍵の部分を格納したパケットを、順次送信するパケット送信手段とを備えて構成することもできる。

【００１１】一方、本発明のパケット受信装置は、前記パケット送信装置からのパケットを順次受信するパケット受信手段と、前記受信した所定数のパケットから前記暗号鍵の部分を抽出する暗号鍵抽出手段と、前記抽出した暗号鍵の部分から元の暗号鍵を生成する暗号鍵生成部と、前記生成された暗号鍵を初期値として疑似乱数列を生成し、該疑似乱数列を用いて前記所定数のパケットに格納される情報の部分を順次ビット単位で復号化するストリーム復号化手段とを備えて構成することができる。

【００１２】

【発明の実施の形態】以下、図示した一実施形態に基いて本発明を詳細に説明する。本発明に係るパケット通信システムは、情報の送信者側におけるパケット送信装置と、情報の受信者側におけるパケット受信装置で構成される。本発明に係るパケット通信システムにおいては、基本的に、パケット内にデータを暗号化するために用いる暗号鍵を格納してデータと共に送信し、該暗号鍵を用いてデータを復号化する手順を取る。以下、この詳細を説明する。

【００１３】図１は、本発明の一実施形態に係るパケット送信装置のブロック図を示している。図において、パケット送信装置１０は、パケット生成部１１、ストリーム暗号部１２、暗号鍵設定部１３、鍵格納部１４及びパケット送信部１５を少なくとも含んで構成される。

【００１４】パケット生成部１１は、送信すべき平文メッセージを複数に分割し、各分割されたメッセージにヘッダーを付加してパケットを生成する。以下では、この分割されたメッセージを平文データ又は単にデータといい、またパケットのこのデータを格納する領域をデータ部という。付加されるヘッダーには、フラグ、送信先アドレス、パケット番号等が含まれる。ストリーム暗号部１２は、ストリーム暗号方式によって前記生成されたパケットのデータ部を暗号化する。ストリーム暗号部１２の具体的な構成及び動作については後述する。暗号鍵設定部１３は、ストリーム暗号部１２における暗号化に用いられる暗号鍵を設定する。暗号鍵設定部１３には、予め複数種類の暗号鍵が用意され、これらは暗号化するパケット毎に切り替えられる。これによって、連続するパケットの各データ部は、ストリーム暗号部１２において、それぞれ異なる暗号鍵を用いて順次暗号化されることとなる。

【００１５】鍵格納部１４は、ストリーム暗号部１２で用いられた暗号鍵を、対応のパケットに格納する。すなわち、鍵格納部１４は、ストリーム暗号部１２で用いられた所定の暗号鍵で暗号化されたデータを含むパケットに、その暗号鍵を格納する。図４は、送信すべきパケットデータの構成例を示している。図に示すように、データ部１の暗号化に用いられた暗号鍵Ａは、そのパケット４０に格納される。同様に、データ部２の暗号化に用いられた暗号鍵Ｂは、そのパケット４１に格納され、データ部３の暗号化に用いられた暗号鍵Ｃは、そのパケット４２に格納される。パケット送信部１５は、前記生成されたパケットを順次ネットワーク上へ送信する。

【００１６】図２は、前記ストリーム暗号部１２の具体的構成例を示すブロック図である。図に示すように、ストリーム暗号部１２は、ｎビットの線形フィードバックシフトレジスタ２０、非線形関数回路２１及び排他的論理和回路２２を備える。線形フィードバックシフトレジスタ２０には、その初期値として前記暗号鍵設定部１３からのｎビットの暗号鍵が設定される。クロック信号に同期してこのレジスタ値は、シフトされ変化される。前記クロック信号に同期してレジスタ値が変化される度に、その各ビット値は、非線形関数回路２１にパラレルに入力される。非線形関数回路２１では、入力されたビット列を非線形変換し、クロック毎に１ビットを疑似乱数として出力する。出力された疑似乱数は、排他的論理

和回路２２に与えられる。従って、一つのレジスタ値に対して、一つの疑似乱数が得られ、線形フィードバックシフトレジスタ２０のレジスタ値がｎビットシフトされた時点で、ｎ個の疑似乱数の組（以下、疑似乱数列という）が出力される。

【００１７】排他的論理和回路２２には、クロック信号に同期して、パケット生成部１１からのｎビットの平文データと前記擬似乱数列が、ビット単位で入力される。平文データの各ビットは、順次擬似乱数列の各ビットと排他的論理和演算され、それが暗号化データの１ビットとして出力される。ｎビットのデータに対し、順次排他的論理和演算が終了することによって、ｎビットの暗号化データが得られる。

【００１８】図３は、メッセージの受信側に設置される本発明の一実施形態に係るパケット受信装置のブロック図を示している。図において、パケット受信装置３０は、パケット受信部３１、暗号鍵抽出部３２、暗号鍵設定部３３及びストリーム復号部３４を少なくとも含んで構成される。

【００１９】パケット受信部３１は、前記パケット送信装置１０からのパケットを順次受信する。受信されたパケットは、図示しないバッファに一時的に保持され、後の処理、すなわち復号化のために待機状態とされる。暗号鍵抽出部３２は、前記受信したパケットの中から暗号鍵を抽出するものである。暗号鍵抽出部３２によって順次抽出された暗号鍵は、暗号鍵設定部３３に格納される。

【００２０】ストリーム復号部３４は、受信した各パケット内のデータ部を復号化する。ストリーム復号部３４は、図２に示したストリーム暗号部１２と同じ構成の復号化手段であり、その線形フィードバックシフトレジスタ２０の初期値として、前記暗号鍵設定部３３の暗号鍵、すなわちパケットに格納された暗号鍵を用いる。図２の排他的論理和回路２２には、非線形関数回路２１の出力と、受信したパケット内の暗号化されたデータが入力され、排他的論理和演算される。これによって、暗号化されたパケット内のデータは、順次復号化され、元の平文データが得られることとなる。この場合に、各パケットのデータは異なる暗号鍵を用いて暗号化されているが、暗号鍵設定部３３は、各パケットの復号化毎にそれに対応した暗号鍵を設定する。ストリーム復号部３４に、複数のパケットの暗号化データが入力され、順次復号化されることによって、元の平文メッセージが完成する。

【００２１】以上のように、パケット内にデータの暗号化に用いた暗号鍵をその暗号化データと共に格納することによって、受信者側における鍵管理が不要になると共に、各パケット毎に用いられる暗号鍵が変えられているので、全体としての暗号強度を高められる。

【００２２】図５～図８は、本発明の他の実施形態に係るパケット通信システムに関するものである。本実施形態に係るパケット通信システムにおいては、複数のパケット毎に、用いる暗号鍵を変更し、その暗号鍵を該複数のパケットに分割して格納し、これを送信する。本実施形態においてそのパケット送信装置は、図１に示した先の実施形態における送信装置と基本的に同じ構成を有するが、暗号鍵設定部１３及び鍵格納部１４の構成において相違がある。すなわち、本実施形態において暗号鍵設定部１３は、所定数のパケット毎にストリーム暗号部１２に設定する暗号鍵を変える。従って、該所定数のパケット内のデータ部は、同じ暗号鍵を用いて暗号化される。

【００２３】図５は、本実施形態における鍵格納部のブロック図を示している。本実施形態において鍵格納部５０は、メッセージダイジェスト生成部５１、暗号鍵分割部５２及び分割鍵格納部５３を備える。メッセージダイジェスト生成部５１は、入力した暗号鍵のビット列から、ハッシュ値その他のメッセージダイジェストを生成し、これを暗号鍵ビット列の後に付加する。ここで、メッセージダイジェストは、元のデータ、すなわち暗号鍵ビット列に実質的に１対１の関係を持つ固定長データである。メッセージダイジェスト生成部５１からは、暗号鍵ビット列にメッセージダイジェストが付加されたものが出力される。暗号鍵分割部５２は、前記メッセージダイジェスト生成部５１の出力ビット列を、所定数に分割する。以下では、この分割されたビット列を分割暗号鍵という。分割暗号鍵の数は、その対応するパケットの数、すなわち分割暗号鍵の元となる暗号鍵を用いて暗号化されたパケットの数に対応する。分割鍵格納部５３は、これらの分割暗号鍵を対応する所定数のパケットに分割して格納する。

【００２４】図６は、前記鍵格納部５０における処理を示した図であり、ここに暗号鍵が分割され複数のパケットに分けて格納される様子が示されている。この例では、ｎビットの暗号鍵に基づいて、ｍビットのメッセージダイジェストが生成され、暗号鍵に付加されている。メッセージダイジェストを付加した暗号鍵のビット列は、この例では、３つに分割され、それぞれ３つのパケットに分けて格納されている。

【００２５】図７は、本実施形態におけるパケット受信装置のブロック図を示している。パケット受信装置７０において、パケット受信部７１、暗号鍵抽出部７２、暗号鍵設定部７３及びストリーム復号部７４は、先の実施形態における対応する構成と同じ機能を有するので、ここではその説明を省略する。パケット受信装置７０は、前記各構成に加え、暗号鍵生成部７５を有している。暗号鍵生成部７５は、前記同じ暗号鍵で暗号化されたデータを含む複数のパケットから抽出された分割暗号鍵から、元の暗号鍵を生成するためのものである。

【００２６】図８に暗号鍵生成部７５の具体的構成例を

示した。すなわち暗号鍵生成部７５は、分割暗号鍵を保持する記憶部８０、１つの暗号鍵を構成する分割暗号鍵の組を特定する鍵判定部８１及び該判定に基づいて元の暗号鍵を作り出す暗号鍵構成部８２を備える。暗号鍵抽出部７２によって各バケットから抽出された分割暗号鍵は、記憶部８０に順次保持される。鍵判定部８１は、先頭より前記所定数（図６の例では３つ）の分割暗号鍵を抽出し、このビット列を結合して、メッセージダイジェストのビット長（例ではｍビット）を最後尾から除く。このビット列から先のメッセージダイジェスト生成部と同じアルゴリズムにより、メッセージダイジェストを生成し、除いた最後尾のビット列と比較する。比較の結果、これらが一致すれば抽出された所定数の分割暗号鍵は正しい組であると判断される。これらが一致しない場合、抽出する分割暗号鍵の組を異ならせて同様の処理を実施する。暗号鍵構成部８２では、前記比較の結果が一致する場合に、前記結合したビット列からメッセージダイジェストのビット長を除いたものを暗号鍵として構成し、図７における暗号鍵設定部７３に与える。前記実施形態においては、暗号鍵が複数のバケットに分割して格納され送信されるので、一層暗号強度が高められる。

【００２７】以上、本発明の一実施形態を図面に沿って説明した。しかしながら本発明は前記実施形態に示した事項に限定されず、特許請求の範囲の記載に基いてその変更、改良等が可能であることは明らかである。

【００２８】

【発明の効果】以上の如く本発明によれば、暗号鍵の変更の同期を必要とせずに、暗号鍵の変更を実現することができ、同期のずれの問題やハードウェアの負荷の問題を回避できる。また、本発明によれば、受信側における暗号鍵の管理を不要とすることができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るバケット送信装置のブロック図である。

【図２】図１のストリーム暗号部の具体的構成例を示すブロック図である。

【図３】本発明の一実施形態に係るバケット受信装置のブロック図である。

【図４】送信すべきバケットデータの構成例である。

＊【図５】本発明の他の実施形態における鍵格納部のブロック図である。

【図６】図５の鍵格納部における処理を示した図である。

【図７】本発明の他の実施形態におけるバケット受信装置のブロック図である。

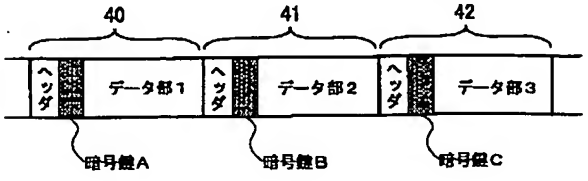
【図８】図７の暗号鍵生成部の具体的構成例を示すブロック図である。

【図９】従来のタイミング信号を用いたバケット通信におけるデータ構成例である。

【符号の説明】

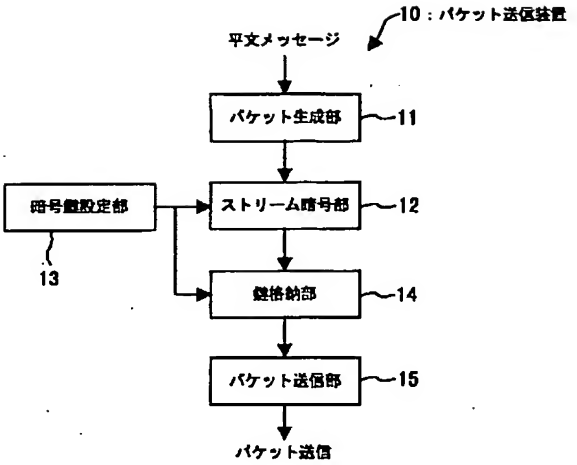
１０　バケット送信装置
１１　バケット生成部
１２　ストリーム暗号部
１３　暗号鍵設定部
１４　鍵格納部
１５　バケット送信部
２０　線形フィードバックシフトレジスタ
２１　非線形関数回路
２２　排他的論理和回路
３０　バケット受信装置
３１　バケット受信部
３２　暗号鍵抽出部
３３　暗号鍵設定部
３４　ストリーム復号部
５０　鍵格納部
５１　メッセージダイジェスト生成部
５２　暗号鍵分割部
５３　分割鍵格納部
７０　バケット受信装置
７１　バケット受信部
７２　暗号鍵抽出部
７３　暗号鍵設定部
７４　ストリーム復号部
７５　暗号鍵生成部
８０　記憶部
８１　鍵判定部
８２　暗号鍵構成部

【図４】

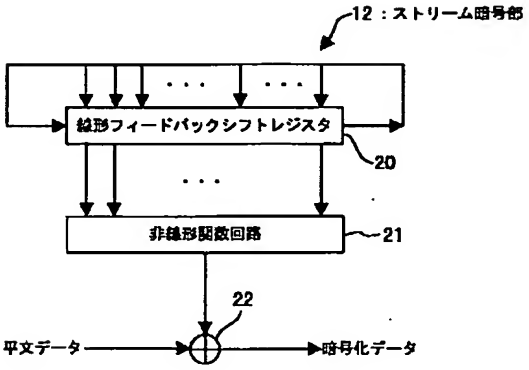


【図９】

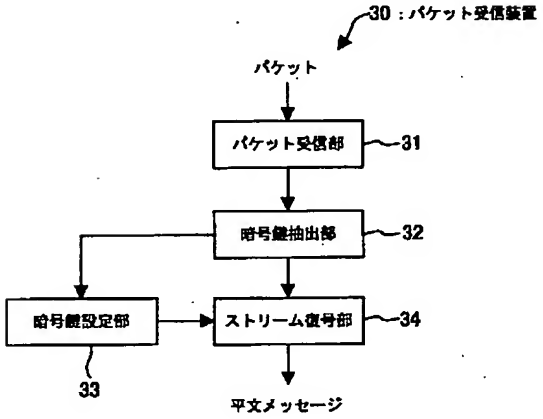
【図１】



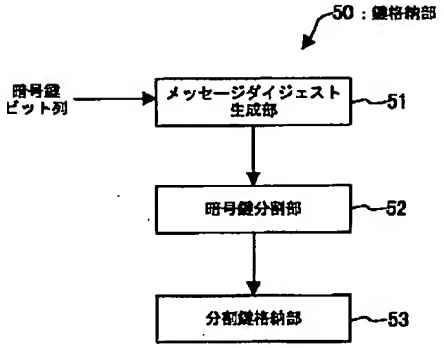
【図２】



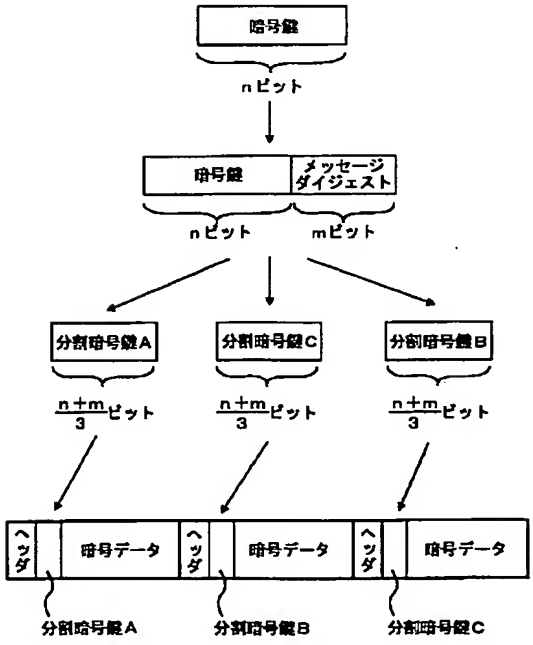
【図３】



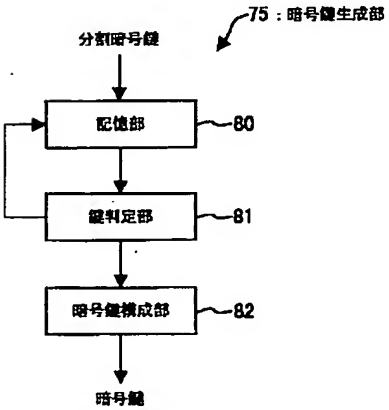
【図５】



【図６】



【図８】



【図７】